UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,198	07/01/2003	Carey Nachenberg	20423-07775	4107

34415 7590 02/08/2008	EXAMINER
SYMANTEC/ FENWICK	DAVIS, ZACHARY A
SILICON VALLEY CENTER	
801 CALIFORNIA STREET	
MOUNTAIN VIEW, CA 94041	

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
02/08/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/612,198	NACHENBERG ET AL.
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-21* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some *   c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   A notice of appeal and pre-appeal brief request for review were received on 15

June 2007.

Response to Arguments

2.   In view of the pre-appeal brief request filed on 15 June 2007, PROSECUTION IS

HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the

following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply

under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed

by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and

appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth

in 37 CFR 41.20 have been increased since they were previously paid, then appellant

must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by

signing below:

Nasser Moazzami

Specification

3.   The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, on page 7, line 7, it appears that the reference to "database 5" is intended to refer to "database 1". On page 7, line 26, it appears that "commend" is intended to read "command".

Appropriate correction is required. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

4.   The use of the trademark Java® has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Objections

5.   Claim 10 is objected to because of the following informalities: Claim 10 does not end with a period. Appropriate correction is required.

Claim Rejections - 35 USC § 101

6.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7.   Claim 20 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Specifically, Claim 20 recites an apparatus that includes a "training module" and a "comparison module". However, the present specification states that the various "modules" described throughout the disclosure may be implemented as software only (see page 4, lines 12-15). A module that only includes software *per se* is functional descriptive material, which is not statutory subject matter unless embodied on a computer readable medium. See MPEP § 2106.01.

Claim Rejections - 35 USC § 112

8.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9.   Claims 3, 4, 6, and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 3 depends from canceled Claim 2, which renders the claim indefinite because it is not possible to determine the metes and bounds of the claim. For

purposes of interpreting the prior art, it has been assumed that Claim 3 is intended to depend from Claim 1.

Claim 4 recites the limitation "at least one observed command is from the group of commands comprising a query, an add, a delete, and a modify". This is not a proper Markush group; first, the commonly used language is "is <u>selected</u> from the group" as opposed to "is from the group" as recited in the claim. More significantly, the use of the term "comprising" (as opposed to "consisting of") renders the claim indefinite because it is not clear exactly what is encompassed by the group. See MPEP § 2173.05(h).

Claim 6 recites the limitation "the categories comprise at least one category from the group of categories comprising: canonicalized commands..." This is not a proper Markush group. First, the commonly used language is "is selected from the group" as opposed to simply "from the group" as recited in the claim. More significantly, the use of the term "comprising" (as opposed to "consisting of") renders the claim indefinite because it is not clear exactly what is encompassed by the group. Additionally, because the list does not include a conjunction (e.g. "and") at its end, it is not clear whether the items are listed in the alternative or inclusive as members of the group. See MPEP § 2173.05(h).

Claim 11 recites the limitation "the suspicious activity" in line 3; however, although the claim also recites "suspicious activity is tracked" in line 2, it appears that the latter does not refer to any specific suspicious activity, but only in a general sense, and therefore, it is not clear to which suspicious activity the reference in line 3 is intended to refer.

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11.   Claims 1 and 3-21 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Applicant admitted prior art, in view of Ramarao et al, US Patent Application

Publication 2004/0199647, and Gruper et al, US Patent 7047369.

In reference to Claim 1, Applicant admits as prior art the general use of database

intrusion detection systems (see page 1, lines 4-17 of the present specification).

However, Applicant does not admit the use of real time training of such a database

intrusion detection system.

Ramarao discloses a method in which an intrusion detection system has derived

a set of acceptable commands (see paragraphs 0056-0057, where there is a list of

allowed actions; see also paragraph 0066, where the access control software can be

implemented as part of an intrusion detection system). Therefore, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to

incorporate the access control portion of the intrusion detection system (IDS) of

Ramarao into the admitted prior art database intrusion detection system, because the

application of the general IDS principles disclosed by Ramarao to the admitted prior art

database IDS would yield the predictable result of increasing the security of the admitted prior art database IDS by preventing unauthorized actions (see Ramarao, paragraph 0027). However, Ramarao does not explicitly disclose that commands are observed in real time before deriving the set of acceptable commands.

Gruper discloses a method in which a security system includes a learning mode in which commands are observed in order to compile an enforcement file of acceptable actions (column 5, lines 32-61). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the real-time learning mode of Gruper into the admitted prior art database IDS as modified by Ramarao, in order to allow a system to gradually build up knowledge of what actions are and are not to be allowed (see Gruper, column 5, lines 32-47).

In reference to Claim 3, Official notice is taken that it is well-known in the art to use SQL commands when accessing a database. Therefore, it would have been obvious to one of ordinary skill in the art to apply the method of Claim 1 when SQL commands are being used to provide the security to the database that uses SQL.

In reference to Claim 4, the cited art further discloses at least one command is a query, an add, a delete, or a modify (see Gruper, column 4, lines 49-64, Table 1; see also Ramarao, paragraphs 0004-0005).

In reference to Claims 5-7, the cited art further discloses grouping the commands into categories and updating statistical information in real time (see Gruper, column 5, lines 32-61), where at least one category includes canonicalized commands having

commands stripped of literal field data (see Ramarao, paragraph 0032, where parameters can be configured as variable).

In reference to Claims 8-10, the cited art further discloses auditing and extracting commands by at least one of an API, code injection, patching, or direct integration (Gruper, column 5, lines 7-61) and in-line interception using at least a proxy, firewall, or sniffer (Ramarao, paragraph 0037).

In reference to Claim 11, the cited art further discloses tracking and reporting suspicious activity (Ramarao, paragraph 0066; Gruper, column 4, line 65-column 5, line 6).

In reference to Claim 12, the cited art further discloses that the duration of performing the deriving step is determined by statistical means (Gruper, column 5, lines 38-55).

In reference to Claim 13-15, the cited art further discloses an operational step in which commands that access the database are compared to the set of acceptable commands, a command that does not match a command in the set is flagged as suspicious, and when a command is flagged as suspicious, at least one of an alert, denial of access, limited access, and investigation is performed (see Ramarao, paragraphs 0066, 0056-0057; see also Gruper, column 4, lines 18-30, and column 4, line 65-column 5, line 6).

Claims 16-19 are directed to software implementations of the methods of Claims 1, 5, 7, and 13, respectively, and are rejected by a similar rationale.

Claim 20 is directed to an apparatus that corresponds substantially to the method

of Claim 1, and is rejected by a similar rationale.

In reference to Claim 21, Applicant admits as prior art the general use of

database intrusion detection systems (see page 1, lines 4-17 of the present

specification). However, Applicant does not admit the use of real time training of such a

database intrusion detection system.

Ramarao discloses a method in which an intrusion detection system has derived

a set of acceptable commands (see paragraphs 0056-0057, where there is a list of \

allowed actions; see also paragraph 0066, where the access control software can be

implemented as part of an intrusion detection system) and that during an operation

phase, commands that access the database are compared to the set of acceptable

commands, and a command that does not match a command in the set is flagged as

suspicious (paragraphs 0066, 0056-0057) and that commands in the set of acceptable

commands can be stripped of literal field data to produce canonical forms and can be

grouped accordingly (paragraph 0032, where parameters can be configured as

variable). Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to incorporate the access control portion of the intrusion

detection system (IDS) of Ramarao into the admitted prior art database intrusion

detection system, because the application of the general IDS principles disclosed by

Ramarao to the admitted prior art database IDS would yield the predictable result of

increasing the security of the admitted prior art database IDS by preventing

unauthorized actions (see Ramarao, paragraph 0027). However, Ramarao does not

explicitly disclose that commands are observed in real time before deriving the set of

acceptable commands.

Gruper discloses a method in which a security system includes a learning mode

in which commands are observed in order to compile an enforcement file of acceptable

actions (column 5, lines 32-61). Therefore, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to incorporate the real-time

learning mode of Gruper into the admitted prior art database IDS as modified by

Ramarao, in order to allow a system to gradually build up knowledge of what actions are

and are not to be allowed (see Gruper, column 5, lines 32-47).

Conclusion

12.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

     a.   Jacobs et al, US Patent 5694595, discloses a management system that

includes checking for valid actions for SQL database structures.

     b.   Gaines, US Patent 5961582, discloses a system in which access is

controlled to a SQL database where database commands are checked for

validity.

     c.   Gleichauf et al, US Patent 6282546, discloses a system for real-time

insertion of data into an intrusion detection system.

d.   Reshef et al, US Patent 6321337, discloses a network security system having access control tests including a list of valid users and actions.

e.   Hemsath, US Patent 6851113, discloses a system for access control that includes a security policy containing a list of allowed actions.

f.   Neufeld et al, US Patent 7240201, discloses a method for secure communications involving a database having a list of allowed commands.

g.   Cohen et al, US Patent 7296274, discloses a system including intrusion detection having a set of allowed actions that can be adapted in real time and/or learned.

h.   Carley, US Patent Application Publication 2003/0233583, discloses a secure appliance that authenticates commands by comparing received commands to an allowed list.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

zad

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100